WE CLAIM:

1. A method of conducting an electronic transaction over a public communications network with an account number, comprising:

generating a per-card key associated with said account number;

generating a message authentication code using said per-card key;

converting said message authentication code into a pseudo expiration date;

generating an authorization request for said transaction, said request having an expiration date field containing said pseudo expiration date; and

verifying said message authentication code based on said pseudo expiration date.

2. The method of claim 1 wherein said electronic transaction is conducted over a public communications network and a payment network including an issuer of said account number, and wherein said account number has a real expiration date, further comprising the steps of generating a second authorization request including said real expiration date and forwarding said second request to said issuer for approval of said transaction.

3. A method of conducting an electronic transaction over a public communications network with a payment account number having an associated pseudo account number, comprising:

(a) generating by a service provider a per-card key associated

with said pseudo account number using said payment account number and said pseudo account number;

(b) creating a secure payment application for use in said transaction including said per-card key;

(c) using said per-card key to generate a message authentication code ("MAC");

(d) generating a MAC verification request by said secure payment application including said pseudo account number and said MAC;

(e) verifying said MAC;

(f) based on said verification, creating an expected transaction sequence number (ETSN) for said MAC;

(g) providing said secure payment application with reference data;

(h) creating a second message authentication code using said expected transaction sequence number and said per-card key;

(i) converting said second message authentication code into a pseudo expiration date using said reference data;

(j) generating an authorization request having an expiration date field containing said pseudo expiration date; and

(k) responding to said authorization request and verifying said second message authentication code based on said pseudo expiration date.

4. The method of claim 3 wherein said per-card key is generated using a per BIN key.

5. The method of claim 2 wherein said MAC verification request further includes an expiration date of said payment account number, a version number and a transaction sequence number value, and wherein said step of verifying said MAC is based on said expiration date, said version number and said transaction sequence number value.

6. The method of claim 5 wherein said step of creating said second message authentication code uses said version number.

7. The method of claim 3 wherein said reference data includes a reference date and a number of months indicator.

8. The method of claim 3 wherein said step of verifying said second message authentication code includes the following steps:

determining said payment account number using said pseudo account number and a stored conversion table;

determining said per-card key associated with said pseudo account number using said payment account number and said pseudo account number;

selecting a second expected transaction sequence number for which an associated message authentication code has not been verified;

converting said third message authentication code into a second pseudo expiration date using second reference data, said second reference data being

specified for said second expected transaction sequence number;

comparing said second pseudo expiration date with said pseudo expiration date; and

verifying said second message authentication code based on said comparison.

9. The method of claim 8 wherein said second message authentication code is verified if said second pseudo expiration date matches said pseudo expiration date.

10. A method of conducting an electronic transaction over a public communications network, with a payment account number having an associated pseudo account number, comprising:

(a) providing said pseudo account number with a control field indicating one of a plurality of key-generation processes to be used to generate an authentication key;

(b) generating an authentication key associated with said pseudo account number using said one of said plurality of key-generation processes indicated in said control field of said pseudo account number;

(c) using said authentication key to generate a message authentication code specific to said transaction;

(d) generating an authorization request message including said message authentication code and said pseudo account number; and

(e) verifying the message authentication code using said indicated key-generation process and said authentication key.

11. The method of claim 10 wherein said authentication key is generated also using an authentication key derivation key on said pseudo account number.

12. The method of claim 11 wherein said authentication key is generated also using a per-BIN key.

13. A method of conducting an electronic transaction over a communications network with an account number, comprising:

generating a per-card key associated with said account number;

generating a message authentication code using said per-card key;

providing at least two different operating modes for forwarding in different manners said message authentication code with an authorization request having different fields, at least one of said operating modes for forwarding said message authentication code in an expiration date field and at least one of said operating modes for forwarding said message authentication code in a message authentication code field.

14. The method of claim 13, wherein said message authentication code is automatically conveyed in said message authentication code field if said message authentication code field exists.